WEST

Freeform Search

Database: US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Term: L8 and ((attribut$ or rule$ or provision$) same (access$ adj3 control$))

Display: 10 **Documents in Display Format:** KWIC **Starting with Number** 1

Generate: ○ Hit List ◉ Hit Count ○ Side by Side ○ Image

Search | Clear | Help | Logout | Interrupt

Main Menu | Show S Numbers | Edit S Numbers | Preferences | Cases

Search History

DATE: Thursday, June 12, 2003 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=YES; OP=ADJ			
L9	L8 and ((attribut$ or rule$ or provision$) same (access$ adj3 control$))	5	L9
L8	L7 and L5	8	L8
L7	L1 and (resource$ with (access$ adj2 control$))	355	L7
L6	L1 and (resource$ and (access$ adj2 control$))	2963	L6
L5	L1 and (resource$ adj3 provider$)	97	L5
L4	L2 and L3	0	L4
L3	L1 and (resource$ and (access$ adj2 control$)).ab.	66	L3
L2	L1 and (resource$ adj3 provider$).ab.	15	L2
L1	(709/$ OR 707/$ OR 705/$).CCLS.	31831	L1

END OF SEARCH HISTORY

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 5 of 5 returned.

☐ 1. Document ID: US 6480861 B1

L9: Entry 1 of 5 File: USPT Nov 12, 2002

DOCUMENT-IDENTIFIER: US 6480861 B1
TITLE: Distributed adaptive computing

Brief Summary Text (13):
Pursuant to one common prior art approach, the management of access to system resources in a distributed environment may be conducted by ascertaining the rights and privileges of a service requestor at the time that a service request is received. If a requestor's privileges are sufficient to allow execution of the request for service provision, the request proceeds. Requestors with insufficient privileges are not granted access to a service. Using this approach, access to a system resource is binary: based upon the identity of the service provider, the request is either granted or not granted. Access privileges to system resources are typically defined and assigned by an administrator. The administrator grants these privileges to requesting entities in an effort to anticipate access requirements in advance of actual service requests. While this method of access control is well-suited to the provision of system security, it is deficient when applied to resource allocation. The assignment of privileges to regulate access to resources is essentially an effort to early-bind the set of resources to a service requestor. Such an assignment shares the same set of design deficits as the early binding technique described above.

Brief Summary Text (15):
Other prior art approaches have dealt with selecting appropriate physical locations for applications on a network so as to enhance system performance. The physical location of an application on a network directly impacts the response time of that application. Services installed on under-utilized resources execute faster than identical services installed on busy resources. The topological proximity of a service to its potential requestors and the proximity of system resources necessary for the delivery of that service directly affect the response time of that service. Ideally, the decision of where an instance of a service ought to be installed takes into account the location of the community of service requestors, available bandwidth, the proximity of data and third party services, and the load on the server where the services run. At present, this decision is typically made by system administrators and is adjusted as new applications, resources and demands are made of the system. Unfortunately, as in the case of resource allocation, decisions pertaining to resource location are also labor-intensive and subject to similar constraints. However, the locations of system resources, service providers, and service points are not readily changeable so as to provide for optimization under a variety of conditions. This is compounded by the difficulty associated with gathering statistics and measures to determine if the location of a service is inefficient and if so, where to relocate the service in order to maximize efficiency.

Current US Original Classification (1):
707/103Y

Current US Cross Reference Classification (1):
705/400

Current US Cross Reference Classification (2):
705/80

Current US Cross Reference Classification (3):
707/10

Current US Cross Reference Classification (4):
709/202

☐ 2. Document ID: US 6460082 B1

L9: Entry 2 of 5 File: USPT Oct 1, 2002

DOCUMENT-IDENTIFIER: US 6460082 B1
TITLE: Management of service-oriented resources across heterogeneous media servers using homogenous service units and service signatures to configure the media servers

Brief Summary Text (26):
It is also an object of the present invention to allow the meta-resource to remain autonomous. Thus, according to the principles of the invention, by providing application-level access control onto a meta-resource, the autonomy of meta-resources is preserved. To this end, each service unit is associated with metadata referred to as a "service signature" which is implemented to customize the service commitment of a meta-resource, e.g., by delivering hints to the meta-resource about resource management. For example, the service signature could be used to define access rights and characteristics for any particular service unit. Similarly, the service signature may recommend run-time compensation strategies to be used to update the resource envelope for this service unit under this meta-resource type at different loads. Thus, the service signature is one of the ways in which the present invention allows the integration of service management with resource management.

col 5 l 39

Detailed Description Text (15):
Similarly, a skilled artisan will appreciate that the meta-resource needs to be trusted by the remote authority and vice-versa. Security when accessing a meta-resource is important to the content subscriber. A mechanism is needed to enforce trust between the different parties. According to today's best practices, a key-exchange mechanism such as RSA may be used to handshake with a resource provider and authenticate the resource provider. Such mechanism is applicable to any other party. Security about the content being accessed is additionally important to the content provider. Thus, enforcement of copyrights and other forms of intellectual property protection over content is necessary. A skilled artisan will appreciate that this is a recognized need and means may be deployed to facilitate the enforcement of copyright between parties having different levels of trustiness. In particular, digital watermarking techniques may be used for safeguarding the copyrights of service objects.

col 10 l 42-51

Detailed Description Text (25):
Via access controls over capabilities and service units, the resource provider is now enabled to grant or deny access to the download of capabilities as well as the administration and configuration of its resources into service units.

col 13 l 28-31

Detailed Description Text (30):
FIG. 8(a) is a flow chart depicting in greater detail the process for handling a provisioning request (800). As shown in FIG. 8(a), the signaling adapter receives the provisioning request and then forwards any such request to the SUMM which then interfaces to the service unit database in order to retrieve and update resource

envelopes (805). At step (810), the service unit signature for the particular requested service is compared with resources at a particular server. Specifically, when a request arrives at the meta-resource, it is necessary to determine whether the request can be serviced, i.e., if the meta-resource is capable, has the resources, is willing to, and has the necessary capability. All these decisions are abstracted by the service unit. Therefore, a determination is made at step (815) as to whether a service unit in a meta-resource is present indicating that the server is capable of provisioning such unit, i.e., that the necessary resources are present. The presence of a service unit provides the ability to determine the willingness of the server in accepting a request. If the service unit is not present, the request fails and the process ends without fulfillment of the request. If the service unit is present, then at step (820) a determination is made as to whether the meta-resource is willing to accept the request, i.e., if the server is willing to provide the media service when criteria such as price, current service unit utilization, and access controls, for example, are considered. Specifically, after a request arrives to the meta-resource, the meta-resource must decide whether to service the request or not. Such decision is supported by the meta-data in the resource. For example, the meta-resource (i.e., the server) determines whether the requests is associated with the right access controls (permissions) to use the service/storage bins being requested. Other criteria are price/cost admissibility. For example, the request may bound cost to $4.00 for example, whereas the meta-resource is willing to provide the service at $3.00. At step (825) the process will terminate if the request is not admissible, or, will continue otherwise. At step (835) any resource envelope adjustments are made and, at step (840), the adjusted service unit is allocated. For example, a service request may request a service unit (X, Y, Z) resource units of respective resources and is currently being serviced. A second request requests (X, Y, Z). For the adjustment step (835), a heuristics database look-up is performed and a determination made as to the form of the resulting resource allocation (f(X), g(Y), h(Z)) given the class of server (meta-resource). Once the resources are determined, any extra resources can be transferred to the overflow pool (e.g., for the duration associated for the provisioning of this request). This is accomplished during step (840) as well. Then, at step (850) the resource monitors are invoked by the operating system of the provisioning meta-resource (server) to monitor actual resources utilized in the provisioning of the requested service which is provided to the client as indicated at step (855). After provisioning of the service, the process ends at step (860) and returns to process more requests at step (865). Typically, the SUMM (FIG. 7) renders all its comparisons and determinations based on the corresponding resource envelope associated with a particular request and then requests the coordination and allocation of the service unit. However, the coordination between the various resources associated with a particular service unit is provided by the coordinated resource management module (730). In turn, the coordinated resource management module interfaces with the resource management interfaces (750) provided by the operating system found on the meta-resource.

Current US Original Classification (1):
709/226

Current US Cross Reference Classification (1):
709/223

Current US Cross Reference Classification (2):
709/224

Current US Cross Reference Classification (3):
709/225

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

☐ 3. Document ID: US 6408336 B1

DOCUMENT-IDENTIFIER: US 6408336 B1
TITLE: Distributed administration of access to information

Drawing Description Text (16):
FIG. 15 is a schema of the part of access control database 301 that defines sites in the VPN and the servers, services, and resources at each site;

Detailed Description Text (84):
col 7 ll 9-15
Thus, in FIG. 4, access filter 403(1) uses its own copy of access control database 301 to determine whether the user who originates a session has access to the information resource specified for the session. If access filter 403(1) so determines, it authenticates the session's outgoing messages and encrypts them as required to achieve the proper trust level. Access filters 403(2..5) then permit the session to proceed because the session is from access filter 403(1) and has been encrypted with SKIP and neither decrypt the messages nor check them using their own copies of access control database 301. Access filter 403(5) then decrypts the messages, confirms that they were encrypted and therefore checked by access filter 403(1), and if the messages are intact, forwards them to server 407 that contains the desired resource. Messages in the session which pass between server 407 and user system 401 are treated in the same way, with access filter 403(5) encrypting them if necessary, access filters 403(2..4) passing them through on the basis of the authentication by 403(5), and access filter 403(1) passing the message on to system 401 on the basis of the authentication and decrypting the message if necessary.

Detailed Description Text (92):
col 8 ll 63 col 9 ll 9
An important task in access control in a VPN is determining the minimum amount of security needed by a session. This is important first because at least that minimum must be guaranteed and second because more security than is necessary wastes resources. The techniques employed in access filters 203 to determine the minimum amount are collectively termed SEND (Secure Encrypted Network Delivery). In SEND, access control database 301 contains a data sensitivity level for each information resource. The data sensitivity level indicates the level of secrecy associated with the information resource and is assigned to the information resource by the security administrator responsible for the resource. An exemplary set of levels is Top Secret, Secret, Private, and Public.

Detailed Description Text (120):
FIG. 7 provides an example of how the sensitivity level of an information resource, the trust level of the user identification, and the trust level associated with the path between the client and the server affect access by the user to the information resource. In FIG. 7, a SKIP-equipped user at client 703 initiates a session 701 to obtain an information resource 723 which is stored at SKIP-equipped server 705. Segment (a) of the above discussion appears in FIG. 7 at 707; segment (b) appears at 709(1..4); Segment (c) appears at 711. Information resource 723 has a sensitivity level of "secret". The first access filter 203 that the session encounters is filter 203(1). Access filter 203(1) uses its copy of the access control database to determine the sensitivity level of resource 723. Here, the user has used a SKIP certificate and an examination of SEND table 601 in data base 301 shows access filter 203(1) that this kind of user identification meets the requirements for information resources having the "secret" sensitivity level, so segment (a) 707 has the required trust level. Consequently, the first access filter goes on to determine the trust level of segments (b) 709(1..4) and (c) between access filter 203(1) and server 705 in the VPN. Segment 709 has subsegments 709(1), 709(2), 709(3), 709(4), and 709(5), and first access filter 203(1) checks the trust level of each of th subsegments in database 301. Segment 709(2) is Internet 121, so its trust level is "public", which is the minimum in segment 709. Then access filter 203(1) uses access control data base 301 to check the trust level of segment 711. It is "secret". Thus, only segment (b) 709 has a trust level that is too low for the path of a session that is accessing a "secret" information resource 703. To deal with this problem, access filter 103(1) must encrypt the session to bring it up to the necessary trust level. First access filter 203(1) consults SEND table 601 to determine what kind of encryption is required, and row 609(2) indicates that DES encryption is sufficient.

First access filter 203(1) accordingly encrypts the session using that algorithm and sends it to access filter 203(5).

Detailed Description Text (148):
As will be explained in more detail later, all access filters 203 have a layered architecture. The bottommost layer is an Internet packet filter 2419 that deals only with Internet packet headers. Packet filter 219 reads the source and destination addresses in the Internet packet headers and applies a set of rules to them. As determined by the rules, it either accepts them, discards them, or routes them further in VPN 201. The rules also determine how the accepted packets are to be routed within access filter 203. The next layer of the architecture is service proxies 2427. The service proxies intercept traffic for services such as the World Wide Web and do access checking on the traffic. If access filter 203 provides the service itself or does access checking for a server that provides the service, IP filter 2419 sends packets intended for the service to a service proxy 2427 for the service. The service proxy uses access control database 301 to do protocol-level access checking for the service. For example, the service proxy for the Web service may check whether the user making a request for a given Web page has access rights for the page. The next higher level is services level 2425; if the relevant service proxy permits an access request and the access filter is also the server for the service, the request goes to the service at service level 2425 to be processed. In the case of the Web page, the service would locate the page and return it to the requester. Two services are involved in the IntraMap: the Web service and an IntraMap service. In FIG. 2401, the Web service appears as WebS 2423. The proxy for WebS 2423 is WebP 2421; for reasons that will become clear in the following, the IntraMap service has only a proxy, IntraMapP 2417. Additionally, access control database 301 includes IntraMap information 2422, which is an optimized version of the information in access control data base 301 that serves as a basis for the IntraMap display.

Detailed Description Text (151):
When the request is received in access filter 203(c), IP filter 2419 forwards it to Web proxy 2421, which in turn forwards it to Web server 2423, which responds to the request by downloading IntraMap applet 2411 to Web browser 2429 in work station 2403, where IntraMap applet 2411 begins executing in Web browser 2429. During execution, it sends a request to IntraMap proxy 2427 for IntraMap information 2422. Like all Java applets, IntraMap applet 2411 sends the request to the server that it is resident on, in this case, access filter 203(c). However, as with any other request from workstation 2403, the request goes by way of local access filter 203(I). There, IntraMap proxy 2427 detects that the request is addressed to IntraMap proxy 2427 in access filter 203(c) and instead of sending the request on to access filter 203(c), obtains IntraMap information 2422 from the local copy of access control data base 301 in local access filter 203(I), filters it so that it specifies only those resources belonging to the information sets to which the user groups to which the user belongs have access to make to list 2431 and returns it via LAN 213 to IntraMap applet 2411, which then uses list 2431 to make IntraMap display 1801. In making the display, applet 2411 applies any filters specified in the request and also sorts the list as specified in the request. List 2431 not only indicates the resources that are available, but also contains information needed to fetch the resource. Thus, if the resource has a hyperlink, the hyperlink is included in the list; if it is a resource for which the user presently does not have access, but to which the user may request access, the list includes the name and email address of the administrator for the resource.

Detailed Description Text (160):
FIG. 14 shows the schema 1401 for the tables that define information sets. These tables relate information sets (resource groups in FIG. 14) to the resources that make them up and to the network locations of the resources and also organize the information sets into the hierarchical list of information sets displayed at 1003 of FIG. 10. Each information set in access control database 301 is represented by a table of class resource group 1403. Tables of class resource group are organized into a hierarchy for inheritance and display purposes by tables 1419. The relationship between an information set and the resources that make it up on one hand and the locations in the VPN in which they are stored are established by tables of class resource group elements 1407. A table of class resource group may be linked

to any number of tables of class resource group elements. A table of class resource group elements is linked to any number of tables of the classes Site Elements 1411, Services 1413, and Resources 1409. There is a table of class Resources for every resource represented in database 301. Included in the table are the resource's ID, its name, the ID for the service that provides it, an ID for a definition of the resource's sensitivity level, a description of the resource, the email address of the administrator of the resource and a hidden flag which indicates whether IntraMap should display the resource to users who do not belong to user groups that have access to the resource. The IntraMap interface obtains the information it needs about a resource from the Resources table for the resource.

Detailed Description Text (215):
FIG. 20 is a block diagram of the architecture 2001 of an access filter 203. In the implementation shown in FIG. 20, all of the components of access filter 203 other than NIC cards 2013 are implemented in software. The software of the implementation runs under the Windows NT brand operating system manufactured by Microsoft Corporation. The software components fall into two broad classes: those that run as applications programs at user level 2003 of the operating system and those that run at the kernel level 2005 of the operating system. In general, the programs that run at the kernel level do IP-level access checking and encryption and authentication, while those that run at the user level do application-level access checking. Also included in the user-level components are software that manages access control database 301 and software that produces the MMFs and rules for IP-level access checking from access control database 301. The following discussion will begin with the kernel components, continue with the user-level components related to access control database 301, and will then deal with the components for protocol-level access checking.

Detailed Description Text (221):
IP Filter 2019: The IP filter operates on a set of rules that the rules compiler, a component of database service 2029, makes from the access policies in access control database 301. The basic functions of IP filter 2019 are to:

Detailed Description Text (227):
f. Pass decisions off to pr_ipf (discussed below) upon establishing a new session for which access control cannot be decided strictly by the rules. Typically, this is for sessions that may be allowed by policies or by the VPN tunneling features described previously.

Detailed Description Text (318):
Administrators can employ the graphical user interfaces disclosed herein to administer the access control data base. The clarity and ease of use of these graphical user interfaces makes it easy to delegate administrative authority to non-specialists. When an administrator makes a change in the access control data base, the change is first made in the local copy of the data base for a given access filter and then propagated to the local copies of the other access filters. The local copy of the access control database also makes it possible to efficiently implement a graphical user interface to the virtual private network which shows a user only those resources that belong information sets to which the user groups to which the user belongs have access.

Current US Original Classification (1):
709/229

CLAIMS:

1. An access filter that administers objects including a plurality of information resources and controls access by a user to an information resource of the plurality, the access filter comprising:

access control information including

at least one object that specifies an explicitly-defined set of users,

at least one object that specifies an explicitly-defined set of information

resources,

at least one object that specifies an explicitly-defined access policy, the access policy defining access by a defined set of users to a defined set of information resources, and

at least one object that specifies an explicitly-defined administrative policy the administrative policy defining administrative access by a defined set of users to an object; and

an access checker that responds to a request by a user to access a resource or to administer an object by determining from the access control information whether the requesting user may access the requested resource or administer the requested object, the access checker being one of a plurality thereof in a network, having a local copy of the access control information, and employing the local copy to check access.

3. The access filter set forth in claim 1 wherein:

the user employs a client to request access to the information resource;

the client includes a browser which display; a list information resources accessible to the user according to the access policy; and

the access checker uses the access control information to determine which information resources are on the list for the browser.

23. An access control system that controls access by users to information resources, the access control system comprising:

access control information including

at least one object that specifies an explictly-defined set of users as a subset of another set of users and

at least one object that specifies an explicitly-defined set of information resources as a subset of another set of information resources, the sets of users and the sets of information resources being organized hierarchically according to their subset relations; and

at least one object that specifies an explicitly-defined access policy, the access policy defining access by a defined set of users to a defined set of information resources, an access policy for a given user subset and a given information resource subset applying to user sets that are below the given user set in the given user set's hierarchy and to information resource subsets that are below the given information resource set in the given information resource set's hierarchy; and

an access checker which responds to a request by a user for access to the information resource by determining from the access control information whether the requesting user may access the requested information resource.

36. The access control system set forth in claim 23 wherein the access checker further comprises:

an information resource information provider for a browser employed by the user to view a list of set of information resources accessible to the user, the information resource information provider using the access control information to provide information about which of the sets of information resources are accessible to the user to the browser.

☐ 4. Document ID: US 6397336 B2

L9: Entry 4 of 5 File: USPT May 28, 2002

DOCUMENT-IDENTIFIER: US 6397336 B2
TITLE: Integrated network security access control system

Abstract Text (1):
A network resource security services control system comprises an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism monitors activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and controllably modifies one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (2):
The present invention relates in general to data processing and communication systems, and is particularly directed to a data communication security access control mechanism, that is comprised of an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicates with one or more information resources within the network. The security access control mechanism of the invention includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (5):
As a reduced complexity, non-limiting example, FIG. 1 diagrammatically illustrates a network user workstation 10 which is coupled via a communication link 11 to a local area network (LAN) 20 by way of a LAN interface 13. LAN interface 13 also provides access to an external network, such as a public communication services (PCS) network, including the Internet 30, that provides potential access to any network information resource (e.g., processor-accessible digital database). The local area network 20 to which user 10 is connected customarily includes one or more computer-based units, such as the illustrated workstations 21 and 22, network server 23 and printer 24, which are interconnected via a hub 25. The hub 25 is connected to the LAN interface 13, so that the end user workstation 10 may access any `local` information resource of the LAN 20. In order to connect to the external network 30, the network interface 13 may be coupled through an electronic mail gateway 32 and a modem 33, whereby a dial-up connection may be provided to an Internet connection or other global resource provider 34, through which access to any node in the overall network is achieved.

Brief Summary Text (6):
Because the network provides a potential window into any information resource linked to any of its nodes, it is customary to both wrap or embed all communications in a `security blanket` (some form of encryption) at a communication sourcing end, and to employ one or more permission (authorization and authentication) layers that must be used to gain access to another system resource (e.g., another computer). Once installed, such schemes operate as micro security systems, primarily as binary permission filters--the user is either permitted or denied access to a destination information resource, and are customarily limited to a relatively limited (and often

fixed) set of access permission criteria. Now, while such schemes provide some measure of access control, they do not provide a macro perspective or control of all of the resources for which a given network security system may be configured.

Brief Summary Text (8):
In accordance with the present invention, this problem is effectively remedied by a new and improved network resource security access control mechanism that includes protection control, access control, event management and a pro-active security agent routines integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network.

Brief Summary Text (11):
The event manager may employ a separate set of policy rules that are not known to the user and serve as an additional layer of access control for enhancing the security of the network. Such policy rules are established external to the network and may include a prescribed activity intensity level associated with the number of or total length of time a resource object may communicate with another resource. In the event a policy rule is violated, the event manager may take relatively limited action, such as sourcing a query to the user to provide further authentication or other information, such as a request to the protection control routine to employ an increased level of cryptography complexity associated with a higher network usage level. On the other hand, if the security rule set employed by the event manager classifies excessive user activity as a substantial network security `threat`, it may call up the pro-active security agent routine, so as to impair the user's ability to use the network. The security rules themselves, as objects of the overall security access control system, may be modified or updated, as required to accommodate event changes, without necessarily terminating access to the network.

Detailed Description Text (2):
Before describing in detail the new and improved network resource security access control mechanism in accordance with the present invention, it should be observed that the present invention resides primarily in what is effectively a new and improved data security access control mechanism implemented as an arrangement of abstract security services. These abstract security services include protection control, access control, event management and a pro-active security agent that are integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network. The particular resources and the information they provide, per se, are not considered part of the invention.

Detailed Description Text (4):
Attention is now directed to FIG. 2, which shows a reduced complexity, non-limiting example of an information resource network 100 having a plurality of resource nodes 110, to which one or more information resource objects, such as respective computers 120 used by user's to couple to and process data transported over the network, may be coupled, and communications among which are supervised or controlled by a network resource security services control system 200. As pointed out briefly above, and as will be detailed infra, network resource security services control system 200 communicates with each of resource and communication control objects, and includes a protection control routine 220, and access control routine 230, and event manager 240 and a pro-active security agent routine 250, which interact with one another and with network resources, so as to control the ability of network users to gain access to, transmit and retrieve information with respect to any of the resources of the network.

Detailed Description Text (9):
An object is any potential participant in the system, such as a user, information resource, communication path, protection mechanism (such as a cryptography algorithm or user's authentication procedure within the protection control routine 220), an access control feature of the access control routine 230, etc.

Detailed Description Text (14):

In addition to such usage rules, the event manager 240 may also have a separate set of policy rules that are not known to the user and serve as an additional layer of access control for enhancing the security of the network. Such policy rules may include a prescribed activity intensity level, which is associated with the number of or total length of time a resource object 120i is using the network to communicate with another resource object 120j. The policy rules may be based upon an a priori activity histogram for other users, with which the user/resource object 120i is expected to conform. As an example, should a resource object 120i spend considerably more time communicating with resource object 120j than established by the histogram, this anomaly would be detected as a violation of policy rules and cause the event manager 240 to execute one or more responses that at least temporarily intrude into the user's network/resource object access session.

Detailed Description Text (17):
Moreover, the security rules themselves, being components or objects of the overall security access control system, may be modified or updated, as required to accommodate event changes, without necessarily terminating access to the network. Thus, in the above example of user activity that might otherwise be initially perceived as exhibiting a substantial network/resource security threat, depending upon the user's interactive response, the policy rules may allow for an adjustment to the threat threshold, before permitting or discontinuing further network access. That fact that each of the security system components is tied together through the events manager substantially facilitates integrating the security services control system into the communication control software of any size or type of data communication network.

Detailed Description Text (18):
As will be appreciated from the foregoing description, the network resource security services control system of the present invention provides an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. This security access control mechanism includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Current US Cross Reference Classification (1):
709/229

CLAIMS:

3. The method according to claim 1, wherein step (c) comprises monitoring information generated by events associated with said user's being selectively granted access to said resource in step (b), and wherein step (d) comprises, in response to information generated by said events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, diminishing the ability of said user to access a network resource.

4. The method according to claim 1, wherein said security relationships among said users and resources of said information network include a protection control routine containing a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among said users and resources of said network, and wherein step (d) comprises modifying one or more of said security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to increase the difficulty of said user to access a network resource.

8. The mechanism according to claim 6, wherein step (b) comprises monitoring

information generated by events associated with said user being selectively granted access to said resource in step (a) and, wherein step (c) comprises, in response to information generated by said events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, diminishing the ability of said user to access a network resource.

9. The mechanism according to claim 6, wherein said security relationships among said users and resources of said information network include a protection control routine containing a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among said users and resources of said network, and wherein step (c) comprises modifying one or more of said security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to increase the difficulty of said user to access a network resource.

☐ 5. Document ID: US 6189104 B1

L9: Entry 5 of 5 File: USPT Feb 13, 2001

DOCUMENT-IDENTIFIER: US 6189104 B1
TITLE: Integrated network security access control system

Abstract Text (1):
A network resource security services control system comprises an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism monitors activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and controllably modifies one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (2):
The present invention relates in general to data processing and communication systems, and is particularly directed to a data communication security access control mechanism, that is comprised of an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism of the invention includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (5):
As a reduced complexity, non-limiting example, FIG. 1 diagrammatically illustrates a network user workstation 10 which is coupled via a communication link 11 to a local

area network (LAN) 20 by way of a LAN interface 13. LAN interface 13 also provides access to an external network, such as a public communication services (PCS) network, including the Internet 30, that provides potential access to any network information resource (e.g., processor-accessible digital database). The local area network 20 to which user 10 is connected customarily includes one or more computer-based units, such as the illustrated workstations 21 and 22, network server 23 and printer 24, which are interconnected via a hub 25. The hub 25 is connected to the LAN interface 13, so that the end user workstation 10 may access any `local` information resource of the LAN 20. In order to connect to the external network 30, the network interface 13 may be coupled through an electronic mail gateway 32 and a modem 33, whereby a dial-up connection may be provided to an Internet connection or other global resource provider 34, through which access to any node in the overall network is achieved.

Brief Summary Text (6):
Because the network provides a potential window into any information resource linked to any of its nodes, it is customary to both wrap or embed all communications in a `security blanket` (some form of encryption) at a communication sourcing end, and to employ one or more permission (authorization and authentication) layers that must be used to gain access to another system resource (e.g., another computer). Once installed, such schemes operate as micro security systems, primarily as binary permission filters--the user is either permitted or denied access to a destination information resource, and are customarily limited to a relatively limited (and often fixed) set of access permission criteria. Now, while such schemes provide some measure of access control, they do not provide a macro perspective or control of all of the resources for which a given network security system may be configured.

Brief Summary Text (8):
In accordance with the present invention, this problem is effectively remedied by a new and improved network resource security access control mechanism that includes protection control, access control, event management and a pro-active security agent routines integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network.

Brief Summary Text (11):
The event manager may employ a separate set of policy rules that are not known to the user and serve as an additional layer of access control for enhancing the security of the network. Such policy rules are established external to the network and may include a prescribed activity intensity level associated with the number of or total length of time a resource object may communicate with another resource. In the event a policy rule is violated, the event manager may take relatively limited action, such as sourcing a query to the user to provide further authentication or other information, such as a request to the protection control routine to employ an increased level of cryptography complexity associated with a higher network usage level. On the other hand, if the security rule set employed by the event manager classifies excessive user activity as a substantial network security `threat`, it may call up the pro-active security agent routine, so as to impair the user's ability to use the network. The security rules themselves, as objects of the overall security access control system, may be modified or updated, as required to accommodate event changes, without necessarily terminating access to the network.

Detailed Description Text (2):
Before describing in detail the new and improved network resource security access control mechanism in accordance with the present invention, it should be observed that the present invention resides primarily in what is effectively a new and improved data security access control mechanism implemented as an arrangement of abstract security services. These abstract security services include protection control, access control, event management and a pro-active security agent that are integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network. The particular resources and the information they provide, per se, are not considered part of the invention.

Detailed Description Text (4):
Attention is now directed to FIG. 2, which shows a reduced complexity, non-limiting example of an information resource network 100 having a plurality of resource nodes 110, to which one or more information resource objects, such as respective computers 120 used by user's to couple to and process data transported over the network, may be coupled, and communications among which are supervised or controlled by a network resource security services control system 200. As pointed out briefly above, and as will be detailed infra, network resource security services control system 200 communicates with each of resource and communication control objects, and includes a protection control routine 220, and access control routine 230, and event manager 240 and a pro-active security agent routine 250, which interact with one another and with network resources, so as to control the ability of network users to gain access to, transmit and retrieve information with respect to any of the resources of the network.

Detailed Description Text (8):
The event manager 240 is a routine that monitors network activity, in particular `events` occurring as a result of activity among users and resources of the network. An event is an activity that occurs when a user executes activity in the network, or as a result of exercising or using a resource or object within the system. An object is any potential participant in the system, such as a user, information resource, communication path, protection mechanism (such as a cryptography algorithm or user's authentication procedure within the protection control routine 220), an access control feature of the access control routine 230, etc.

Detailed Description Text (13):
In addition to such usage rules, the event manager 240 may also have a separate set of policy rules that are not known to the user and serve as an additional layer of access control for enhancing the security of the network. Such policy rules may include a prescribed activity intensity level, which is associated with the number of or total length of time a resource object 120i is using the network to communicate with another resource object 120j. The policy rules may be based upon an a priori activity histogram for other users, with which the user/resource object 120i is expected to conform. As an example, should a resource object 120i spend considerably more time communicating with resource object 120j than established by the histogram, this anomaly would be detected as a violation of policy rules and cause the event manager 240 to execute one or more responses that at least temporarily intrude into the user's network/resource object access session.

Detailed Description Text (16):
Moreover, the security rules themselves, being components or objects of the overall security access control system, may be modified or updated, as required to accommodate event changes, without necessarily terminating access to the network. Thus, in the above example of user activity that might otherwise be initially perceived as exhibiting a substantial network/resource security threat, depending upon the user's interactive response, the policy rules may allow for an adjustment to the threat threshold, before permitting or discontinuing further network access. That fact that each of the security system components is tied together through the events manager substantially facilitates integrating the security services control system into the communication control software of any size or type of data communication network.

Detailed Description Text (17):
As will be appreciated from the foregoing description, the network resource security services control system of the present invention provides an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. This security access control mechanism includes monitoring activity associated with user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications

with respect to a system resource.

Current US Cross Reference Classification (1):
709/229

CLAIMS:

5. A method according to claim 1, wherein step (c) comprises monitoring information generated by a plurality of events associated with said network user's accessing said network resource in step (b), and wherein step (d) comprises, in response to information generated by said plurality of events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, decreasing the ability of said network user to access a network resource.

6. A method of controlling the ability of a user to access one or more information resources of an information network comprising the steps of:

(a) providing a protection control routine having a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among users and resources of said network;

(b) selectively permitting a user to access a network resource in accordance with at least one of a plurality of security relationships among users and resources of said information network; and

(c) controllably modifying one or more of said plurality of security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to affect the ability of said user to access a network resource.

Generate Collection | Print

Term	Documents
ATTRIBUT$	0
ATTRIBUT	18
ATTRIBUTABE	1
ATTRIBUTABEL	1
ATTRIBUTABL	3
ATTRIBUTABLE	53643
ATTRIBUTABLES	1
ATTRIBUTABLETO	1
ATTRIBUTABLE-EXCELLENT	1
ATTRIBUTABLE-FOR	1
ATTRIBUTABLLE	1
(L8 AND ((ATTRIBUT$ OR RULE$ OR PROVISION$) SAME (ACCESS$ ADJ3 CONTROL$))).USPT.	5